GENERAL RULES AND GUIDELINES GOVERNING THE USE OF BUREAU OF LAND MANAGEMENT COMPUTER SYSTEMS

According to the Department of Interior Manual 375 DM 19.10B, "*It is the responsibility of each employee to report all suspected, actual or threatened incidents involving automated information systems to the authorities indicated below*."

- **Bureau of Land Management (BLM) employees shall report observed computer security incidents or suspected computer security violations immediately to the Installation Information Technology (IT) Security Manager and to their supervisors.**

- **The BLM Installation IT Security Manager may recommend the removal of any individual's User ID and password from any BLM computer system and/or application system in the event of a security incident.**

- **Unauthorized access or misuse of BLM computer systems may subject violators to criminal, civil or administrative action. Criminal Penalties include fines and/or imprisonment of up to 20 years. Disciplinary action for administrative violations of the following rules may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or other action as deemed appropriate.**

Violations of the following rules are considered computer security incidents:

1. **CLASSIFIED INFORMATION.** No classified National Security information will be entered into any BLM computer system.

2. **GOVERNMENT PROPERTY.** Computer hardware, software, and data of the BLM are considered to be the property of the U.S. Government. BLM computer systems shall be used for official business only. No games, personal software, private data, unlicensed proprietary software, or otherwise non-government information will be used on or entered into any Government-owned computer system. Any use of computers, software or data for other than official business is expressly prohibited, except as permitted by the BLM Internet Acceptable Use Policy.

3. **PROPRIETARY PROPERTY.** Commercially developed and licensed software shall be treated as proprietary property of its developer. Title 17 of the U.S. Code states that "It is illegal to make or distribute copies of copyrighted material without authorization." The only exception is the user's right to make a backup for archival purposes, assuming one is not provided by the manufacturer. It is illegal to make copies of software for any other purpose without permission of the publisher. Unauthorized duplication of software is a Federal crime. Penalties include fines of up to $100,000 per infringement and jail terms of up to 5 years.

4. **ACCOUNTABILITY.** Individual User IDs and passwords shall be assigned only to persons having a valid requirement to access BLM computer systems. All activity accomplished under this User ID is directly attributable to the user to whom it is assigned.

GENERAL BUSINESS PRACTICES, which if not followed can lead to security incidents, are listed below. Noncompliance with these practices may result in removal of access and/or disciplinary or legal action being taken, consistent with the nature and scope of such activity.

1. **INDIVIDUAL USER IDs AND PASSWORDS.** Do not share your individual User IDs and passwords. They are to be used only by the individual owner. User IDs and passwords should not be written down except on the original assignment document. Once memorized, this document should be destroyed or, at a minimum, be kept in a locked safe or cabinet.

   Under no circumstances should User IDs and passwords be posted ANYWHERE! Nor should they be kept in accessible locations. Never use personal information (e.g., telephone numbers, names of family members, pets, etc.) or dictionary words for your passwords. Passwords should be eight characters in length and consist of at least one numeric character, a special character, and both upper and lower case letters. Passwords should be changed at required intervals. If you believe your User ID and password have been compromised, change your password, notify your supervisor, and report the incident to the Installation IT Security Manager.

2. **UNAUTHORIZED ACCESS.** Access to BLM computer systems requires management approval. Do not attempt to gain access to any Information Technology system for which you do not have an approved and authorization to access.

3. **LOG OFF** when not actively working on the computer system. At a minimum, lock your workstation when leaving your work area for short periods of time or invoke the computer system's locking screen saver. **Remember, you are responsible for all activity logged under your User ID.**